علوم رایانش و فناوری اطلاعات
نشریه علمی انجمن کامپیوتر ایران
مجلد ۱۸، شماره ۲، ۱۳۹۹
صفحات ۶۰- ۶۵
مقاله عادی

S-Boxهای پویای وابسته به کلید سبک وزن مبتنی بر خم ابربیضوی برای دستگاه‌های اینترنت اشیا

پروانه اصغری[1*]، سید حمید حاجی سید جوادی[2]

*پروانه اصغری، دریافت: ۱۳۹۹/۰۹/۲۳، بازنگری: ۱۳۹۹/۰۹/۲۸، پذیرش: ۱۳۹۹/۱۰/۱۰

[1]گروه مهندسی کامپیوتر، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
[2]دانشکده علوم، گروه ریاضی و علوم کامپیوتر، دانشگاه شاهد، تهران، ایران

چکیده

موضوع امنیت یکی از اصلی ترین مباحث در محیط اینترنت اشیا است. با توجه به اهمیت نقش موثر روش های رمزنگاری بلوک در ایجاد امنیت در اینگونه سیستم‌ها، تولید S-Box از اهمیت ویژه‌ای در رمزنگاری برخوردار است. با توجه به محدودیت ظرفیت منابع درگره های اینترنت اشیا ، تولیدS-Box سبک وزن یک چالش مهم است. در این مقاله یک روش تغییر در S-Boxهای رمزنگاری متقارن ایستا وابسته به کلید و تولید آنها به شکل پویا با استفاده از خم ابربیضوی[1] ارائه می‌شود. S-Box پیشنهادی با استفاده از معیارهای عملکردی از جمله دو سوئی بودن[2]، غیرخطی بودن[3]، اثر فروپاشی بهمنی[4] و درجه جبری[5] ارزیابی می‌شود. نتایج ارزیابی تائید می‌کند که الگوریتم تولید S-Box ارائه شده یک روش موثر برای تولید S-Boxهای سبک وزن و قوی رمزنگاری است.

کلمات کلیدی: S-Boxپویا، امنیت اینترنت اشیا، رمز بلوکی، خم ابربیضوی

۱- مقدمه

با توجه به نفوذ روز افزون استفاده از اینترنت اشیا (IoT) در بیشتر جنبه‌های زندگی بشر امروزی، ابعاد مختلف استفاده از این بستر، طی سال‌های اخیر مورد توجه جامعه پژوهشگران قرار گرفته است. هنگام استفاده از اینترنت اشیا بخصوص در کاربردهای حساس و بحرانی، بحث امنیت و رمزنگاری اطلاعات به یک ضرورت حیاتی تبدیل می‌شود. دلایل عمده توسعه روش‌های جدید رمزنگاری سبک وزن در محیط اینترنت اشیا عبارت است از الف) محدودیتهای منابع دستگاه‌های اینترنت اشیا به لحاظ حافظه و توانایی پردازش و ب) بهره وری از ارتباطات انتها به انتها[6] که منجر به استفاده از روش‌های رمزنگاری متقارن سبک وزن جهت صرفه‌جویی در مصرف انرژی در منابع اینترنت اشیا با توان پائین با هدف دستیابی به امنیت بیشتر می‌شود [۳-۵].

الگوریتم‌های رمزنگاری سنتی برای استفاده در تلفن‌های همراه و رایانه ها بسیار مناسب هستند، در حالیکه در شبکه‌های اینترنت اشیا، نقاط انتهایی طیف شامل دستگاه‌هایی مانند سنسورها ، برچسب‌های RFID و سیستم‌های جاسازی شده است که این دستگاه‌ها بدلیل محدویت‌های حافظه و ظرفیت محاسباتی، معمولاً به سیستم عامل‌هایی نیاز دارند که از روش‌های رمزنگاری سبک وزن استفاده می‌کنند [۳]. به طور کلی، رمزنگاری سبک وزن، زیرمجموعه‌ای از روش-های رمزنگاری است که تکنیک‌هایی را ارائه می دهد که معمولاً در دستگاه های هوشمند کم مصرف استفاده می‌شوند [۶].

تکنیک‌های رمزنگاری، بطور کلی به عنوان رمز جریانی و بلوکی[7] در نظر گرفته می‌شوند [۷]. روش‌هایAES[8] [۸]، DES[9] [۱] و SMS4 [۹] از گزینه‌های پرکاربرد روش‌های رمزنگاری هستند. S-Box[10] بخش اصلی در رمز بلوکی است و تأثیر مستقیمی بر سطح امنیتی رمزنگاری دارد [۱۱]. به دلیل ماهیت پویای محیط اینترنت اشیا، استفاده از رمزهای بلوکی ایستا کارایی لازم را ندارند. زیرا با توجه به اندازه بزرگ جداول S-Boxهای ایستا که در دستگاه‌های اینترنت اشیا بدلیل محدودیت‌های منابع امکان ذخیره‌سازی آنها میسر نیست، بهتر است از S-Boxها با اندازه جداول کوچک استفاده شود. از سویی دیگر،در Boxهای ایستا، بدلیل ثابت بودن رمزهای بلوکی، S-Boxهای تولید شده نسبت به S-Boxهای پویا، در برابر حملات سریع‌تر و راحت‌تر باز می‌شوند. از این رو با کوچک کردن S-Boxها و تولید S-Boxهای سبک وزن که دارای اندازه جداول کوچکتری هستند و در عین حال پویایی آنها، می‌توان به سطح مناسبی از امنیت در دستگاه‌های با منابع محدود ذخیره‌سازی و محاسباتی دست یافت. بنابراین، پیشنهاد روشی جهت تولید S-Box پویا و سبک وزن یک نیاز حیاتی در محیط اینترنت اشیا است که در

آن شبکه حسگر بی‌سیم[11] شبکه بی‌سیم بدن[12] و کارت‌های هوشمند به کار گرفته می‌شوند.

بررسی‌های انجام شده بر روی مسئله S-Box پویا نشان می‌دهد که S-Box به طور گسترده‌ای بر روی محیط‌های دارای منابع حافظه و محاسباتی با ظرفیت بالا متمرکز شده است. اما هنگامی که اشیا هوشمند با عمر باتری کم، قدرت محاسبه پائین، پهنای باند و حافظه محدود که به ویژه در محیط‌های اینترنت اشیا استفاده می‌شوند، استفاده و بکار گیری S-Boxها به عنوان یک یک چالش مهم مطرح می‌شودکه کاملاً ناشی از توسعه فن‌آوری استفاده از دستگاه‌های مجهز به حسگرها در محیط اینترنت اشیا است [۱۳ ، ۱۴]. با توجه به محدودیت منابع حافظه و منابع محاسباتی در بستر اینترنت اشیا در دنیای واقعی، در این مقاله، بر روی رروش‌های تولید S-Box سبک وزن پویا ، جهت غلبه بر محدویت‌های ذکر شده، تمرکز شده است.

به‌عنوان یکی از روش‌های مطرح در این زمینه، خم ابر بیضوی[13] توسط کوبلیتز [۱۵] برای استفاده در رمزنگاری به عنوان جایگزینی مناسب برای منحنی‌های بیضوی پیشنهاد شد. خم ابربیضوی در گروه منحنی‌های جبری است که به عنوان گسترشی از منحنی‌های بیضوی در نظر گرفته می‌شوند. همچنین، تعریف رمزنگاری خم ابربیضوی بر اساس منحنی‌هایی است که در آنها $g \geq 1$[14] است. آنچه که استفاده از این نوع منحنی را مطلوب می‌کند آن است که خم ابربیضوی، اشیا هوشمند را قادر می‌سازد که به پهنای باند و ذخیره سازی کمتری نیاز داشته باشند [۱۶].

در این مقاله، یک روش جدید تولید S-Box پویا ارائه شده است که در آن بهبود بیشتری در امنیت روش رمزنگاری بلوک سبک وزن نسب به روش مطرح شده در SMS4 که در آن S-Box بصورت ایستا است، حاصل شده است. در این مقاله پس از بیان نحوه ساخت S-Box، به تجزیه و تحلیل آن جهت ارزیابی قدرت رمزنگاری روش پیشنهادی می‌پردازیم. ارزیابی کارایی طرح ارائه شده با انجام فرایندهای شبیه سازی با استفاده از SageMath جهت محاسبه خم ابربیضوی انجام می‌شود و سپس S-Box تولید شده تحلیل و ارزیابی می‌شود [۱۷].

به طور خلاصه، هدف این مقاله ارائه پیشنهادی یک الگوریتم جهت تولید S-Box وابسته به کلید پویا با استفاده از خم ابربیضوی است. به طور خاص ، هدف اصلی ما بهبود امنیت SMS4 از طریق ایجاد S-Box پویا و وابسته به کلید است. به‌عنوان مثال، یک S-Box موجود در SMS4 جدول ۱ نشان داده شده است [۹].

جدول ۱- S-Box در SMS4

x	0 1 2 3 4 5 6 7 8 9 A B C D E F
S(x)	C 5 6 B 9 0 A D 3 E F 8 4 7 1 2

ساختار این مقاله بدین شرح است: در بخش ۲، مفاهیم مقدماتی روش رمزنگاری سبک وزن توضیح داده شده است. کارهای پیشین در بخش۳ مورد بحث و تجزیه تحلیل قرار گرفته است. در بخش ۴، جزئیات طرح پیشنهادی جهت تولید S-Box پویا وابسته به کلید ارائه شده است. در بخش ،۵ به تجزیه و تحلیل الگوریتم پیشنهادی پرداخته شده و در بخش،۶ نتیجه گیری کلی ارائه شده است.

۲- مفاهیم مقدماتی الگوریتم‌های رمزنگاری سبک وزن

به طور کلی الگوریتم های رمزنگاری سبک وزن بر اساس سه مفهوم اساسی بنا شده اند که عبارتند از: رمز بلوکی سبک وزن[15] ، توابع درهم ساز سبک وزن[16] و رمز جریانی سبک وزن[17].

• رمز بلوکی سبک وزن: به طور کلی، رمزنگاری بلوکی یک الگوریتم قطعی در رمزنگاری است که روی مجموعه‌ای از بیت‌ها با طول ثابت به نام بلوک‌ها با یک تغییر ثابت که از طریق یک کلید متقارن مشخص می‌شود، انجام می‌شود. همچنین، رمزهای بلوکی سبک وزن به عنوان عناصر اصلی در توسعه روش‌های مختلف رمزنگاری استفاده می‌شوند و به طور گسترده در انجام رمزنگاری داده‌های انبوه استفاده می‌شوند. به طور معمول، یک رمز بلوکی، از یک جفت تابع شامل تابع رمزنگاریری (E) و تابع رمزگشایی (D) تشکیل شده است. این توابع با ورودی‌هایی که شامل یک بلوک با اندازه n بیت و یک کلید با اندازه k بیت هستند، یک بلوک خروجی با اندازه n بیت تولید می‌کنند. تابع رمزگشاییD به عنوان معکوس تابع رمزنگاری E در نظر گرفته می‌شود (E−1 = D) [۱۹]. توابع رمزنگاری و رمزگشایی رمز بلوکی بوسیله معادلات ۱ و ۲ تعریف می‌شوند [۲۰].

تابع رمزنگاری:

$$E_k(P) := E(K,P) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n \qquad (۱)$$

تابع رمزگشایی:

$$E_k^{-1}(C) := D_k(C) = D(K,C) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n \qquad (۲)$$

تابع رمزنگاری (معادله ۱) ، یک کلید K به طول k و یک بیت رشته P با طول n یک رشته C با اندازه n بیت ایجاد می‌کند. P متن ساده[18]است و C متن رمزنگاری[19] شده است. برای هر کلید K، معادله $E_k(P)$ ، باید یک نگاشت وارون بر روی $\{0,1\}^n$ باشد. در تابع رمزگشایی (معادله ۲) که معکوس E است، ورودی ها از یک کلید K و یک متن رمز دار C تشکیل شده و خروجی یک متن ساده P است، بطوریکه $\forall K: D_k(E_k(P)) = P$.

یکی از اهداف مورد توجه در بستر اینترنت اشیا که منابع ظرفیت محاسباتی و ذخیره‌سازی محدود ی دارند، ایجاد رمزهای بلوکی سبک وزن است که به دلیل اندازه کوچکتر جداول، مناسب اینگونه بسترها هستند. بنابراین، نکات مهمی در ساخت رمزهای بلوکی سبک وزن، باید در نظر گرفته شوند که عبارتنداز:

۱) باید از بلوک‌های با اندازه‌های کوچکتر برای استفاده در رمزنگاری‌های بلوک سبک وزن استفاده شود که این موضوع اندازه متن ساده را محدود می کند.

۲) برای دستیابی به مصرف کمتر انرژی بدلیل عمر محدود باتری، باید از اندازه کلید کوچکتری استفاده شود.

۳) برای انجام مراحل محاسبه ساده‌تر در مقایسه با روش‌های رمزنگاری سنتی، باید چرخش‌های کوتاه‌تری انجام شوند. به عنوان نمونه، S-Boxها با اندازه ۴ بیت در یک S-Box سبک وزن، در مقایسه با S-Box ۸ بیتی در رمزنگاری سنتی، تولید می‌شوند.

۴) برای کاهش حافظه ومصرف کمترانرژی در تولید S-Boxها، باید روش‌های تولید کلید ساده‌تری در نظر گرفته شود زیرا یک رمزنگارز بلوک سبک وزن دارای روش‌های تولید کلیدهای ساده‌تری است که زیرکلیدها را تولید می‌کنند.

• توابع درهم ساز سبک وزن : توابع درهم ساز سبک وزن در مقایسه با تابع درهم ساز معمول که برای دستگاه‌های هوشمند اینترنت اشیا با منابع محدود، مصرف انرژی بالا را به دنبال دارند، به طور گسترده‌ای مورد استفاده قرار گرفته‌اند. اهداف اصلی طراحی توابع درهم ساز سبک وزن شامل موارد زیر است [۱۹]:

۱) اندازه کوچکتر خروجی در کاربردهایی که دارای مقاومت در برابر تصادم تابع درهم‌ساز هستند ، یک ضرورت مهم است. درکاربرد هایی که مقاومت در برابر تصادم ضروری نیست، به طور کلی از اندازه‌های متعادل استفاده می‌شود.

۲) در بستر اینترنت اشیا باید از اندازه پیام کوچکتر استفاده شود. تابع درهم ساز کلاسیک معمولاً از اندازه ۲۶۴ بیت در مقایسه با ظرفیت کمتر تابع درهم ساز سبک وزن، استفاده میکند. بنابراین ، توابع درهم ساز که برای پیام‌های کوچک استفاده می‌شوند، درکاربرد های اینترنت اشیا با ظرفیت محدود مناسب‌ترند.

• رمزنگارهای جریان سبک وزن، باید به عنوان روش‌های اصلی در محیط اینترنت اشیا با منابع محدود در نظر گرفته شوند.

در رمزهای بلوکی، یک S-Box که عنصری اصلی در روش‌های کلید متقارن است، عمل جایگزینی انجام می‌شود. در رمزهای بلوکی معمولاً ارتباط بین متن رمز و کلید ، پنهان می‌شود. به طور کلی ، یک S-Box از مجموعه ای از n بیت به عنوان ورودی استفاده می‌کند و آنها را به مجموعه ای از m بیت به عنوان خروجی تبدیل می‌کند، بطوری که ممکن است m برابر با n نباشد. یک n × m S-Box به صورت یک جدول که شامل 2n کلمه m بیتی است، ساخته می‌شود [۲۱]. بطور معمول در DES، از جدول‌های ثابت استفاده می‌شود، در حالیکه در بعضی از رمزها، جداول به صورت پویا، از کلیدهایی تولیدی با روش‌هایی مانند رمزنگاری Twofish و Blowfish ساخته می‌شوند [۲۲].

۳- کارهای پیشین

در این بخش، به بحث و تحلیل تعدادی از مطالعات و مقالات مرتبط پیشین در رابطه با روش‌های تولید S-Box می‌پردازیم.

در [۲۳] ، نویسندگان روشی را جهت تولید S-Box پویا وابسته به کلید ارائه کردندکه با روش تولید S-Box در AES، به عنوان یک استاندارد و معیار جهت ارزیابی، مورد مقایسه قرار گرفت. روش پیشنهادی بر اساس کلمه رمز [۲۰]تولید شده از کلید، طراحی شده است. همچنین ، کلید استفاده شده برای رمزنگاری با اندازه ۶۴ بیت در نظر گرفته شده است. یک کلمه مانند (C8C7C6C5C4C3C2C1) در زمان اجرا بر اساس فاصله و وزن همینگ کلید تولید می‌شود. این تابع شامل عملیات تغییر سطرها و ستون ها و همچنین مبادله و تبادل عناصر است. نقطه ضعف بارز روش پیشنهادی این است که به دلیل طراحی مشابه AES جهت استفاده در دستگاه‌های با منبع محدود، مناسب نیست.

در [۲۴] ، نویسندگان روشی را برای تولید S-Box وابسته به کلید بر اساس استراتژی AES، از طریق استفاده از چرخش[۲۱] در S-Box ارائه کردند. فرآیندهای رمزنگاری و رمزگشایی در این روش مانند AES استانداردر است ، با این وجود روش موجود در AES استاندارد از چهار مرحله تشکیل شده است در حالیکه روش جدید شامل پنج مرحله است که مرحله اضافه شده در این مقاله شامل چرخش S-Box است و مقدار چرخش حاصل با کل چرخش کلید در رابطه است. محدودیت اصلی این طرح همانند محدودیت در مقاله [۲۳] است.

در [۲۵] ، یک روش جدید تولید S-Box از AES ، با استفاده از روش نگاشت متغیر ارائه شده است. روش پیشنهادی یک روش مبتنی بر AES است که داده کلید برای تولید فاکتوری استفاده می‌شود. در این الگوریتم، از مجموعه داده‌های زیر کلید وابسته به کلید اصلی، جهت نگاشت مجدد و جایگزینی S-Box به یک موقعیت تصادفی استفاده می‌شود. این طرح از چهار چند جمله‌ای غیرقابل کاهش با درجه هشت استفاده می‌کند. تغییرات لازم برای نگاشت معکوس S-Box، رابطه غیر خطی بین S-Box و عکس آن را حفظ میکند. نقطه ضعف این روش همانند ضعف روش ارائه شده در مقاله [۲۳] است.

در [۲۶] ، نویسندگان الگوریتمی جدید برای تولید S-Box پویا از طریق یک فرآیند دو مرحله‌ای معرفی کردند. در مرحله اول، از روش AES برای تولید S-Box استفاده می‌شود و در مرحله دوم، سطرها و ستون ها تبادل می‌شوند. بعلاوه، برای تولید S-Box پویا ، از کلید وابسته استفاده می‌شود. با توجه به روش AES بکار رفته جهت تولید S-Box ، روش پیشنهادی در این مقاله برای دستگاه‌های با منابع محدود مناسب نیست.

همچنین در [۲]، الگوریتمی برای تولید S-Box پویا پیشنهاد شده است که علاوه بر استفاده از سه تابع بازخورد خطی مختلف، از سه ثبات جابجایی[۲۲] با بازخورد خطی استفاده می‌کند.. در خروجی این ثبات‌ها، یک عمل XOR انجام می‌شود و سپس خروجی پویا به ۱۲۸ بیت بلوک مجزا تقسیم می‌شود که از هر بلوک جهت تولید S-Box استفاده می‌شود.

۴- روش پیشنهادی جهت تولید S-Box

در این بخش ، ابتدا زمینه ریاضی روش تولید S-Box وابسته به کلید به طور خلاصه شرح داده می‌شود و سپس روش پیشنهادی مبتنی بر خم ابربیضوی ارائه می‌شود.

۴-۱- مفاهیم ریاضی

جهت روشن شدن مفاهیم اصلی کاربردی در این مقاله ، توضیح مختصری از زمینه ریاضیات مورد نیاز برای توسعه روش تولید S-Box وابسته به کلید ارائه می‌شود. روش پیشنهادی بر اساس تعاریف ارائه شده ۱ و ۲، و ایده خم ابربیضوی، متکی است.

تعریف ۱: یک خم ابر بیضوی C از نوع d بر روی میدان کامل K با مشخصه عدد اول p ، بر اساس معادله ۳ تعریف می‌شود:

$$C: Y2 + H(x)y = F(x) \qquad (۳)$$

در معادله ۳، $H(x)$ یک چند جمله‌ای از درجه d و $F(x)$ یک چند جمله‌ای از درجه $2d + 1$ است [۲۸].

مثال ۱: اگر p =۱۱ باشد، معادله $y2 = x5 + 2x2 + x + 3$ روی میدان کامل K ، یک خم ابربیضوی از درجه ۲ می‌دهد.

با داشتن یک نقطه مانند P از مرتبه n در یک خم ابربیضوی C بر روی میدان متناهی K_a و یک نقطه Q روی C، می‌توانیم یک عدد صحیح m پیدا کنیم بطوریکه $0 \le m \le n-1$ و $Q = m.P$ باشد، به گونه‌ای که Q از ضرب اسکالر m و P به‌دست می‌آید. با دانستن مقادیر P و Q یافتن مقدار m غیرممکن است. به این مشکل، مسأله لگاریتم گسسته خم ابربیضوی (HCDLP) [۲۳] گفته می شود. ایده اصلی در این مقاله از همین چالش به دست آمده است.

فرآیندهای رمزنگاری و رمزگشایی از مجموعه متناهی نقاط بر روی خم ابربیضوی، روی میدان کامل K ، استفاده می‌کنند. از معادله ۳ برای به دست آوردن نقاط مانند P روی منحنی C استفاده می‌شود.

تعریف ۲: مقسوم علیه D از حاصل جمع نقاط در C، بر اساس معادله ۴ به دست می‌آید:

$$D = \sum_{P \in C} m_p . P \quad , m_p \in Z \qquad (۴)$$

در این روش، یک عدد تصادفی به عنوان یک کلید خصوصی در نظر گرفته می‌شود و کلید عمومی Q، با ضرب کلید خصوصی در نظر گرفته شده با یک نقطه مانند P روی منحنی C بدست می‌آید. امنیت تابع رمزنگاری مبتنی بر خم ابربیضوی به سطح پیچیدگی HCDLP بستگی دارد.

کارایی تابع رمزنگاری مبتنی بر خم ابربیضوی، بر اساس محاسبه کارآمد ضرب اسکالر $Q = m.P$ است. تابع رمزنگاری مبتنی بر خم ابربیضوی از کلید با اندازه کوچک استفاده می‌کند که این خود باعث می‌شود در این روش، سطح امنیت مشابه الگوریتم‌های دیگر مانند RSA ارائه شود.

۴-۲- الگوریتم پیشنهادی

فرض کنید H یک خم ابربیضوی است که در یک میدان متناهی K_a با مشخصه $a > 0$ در نظر گرفته می‌شود. فرض کنید که D_m یک مقسوم علیه مرتبه n است. با توجه به D_n، مسأله HCDLP، شامل دستیابی به یک عدد صحیح δ است، بطوریکه $0 \le \delta \le n-1$ ، به گونه‌ای که $D_n = \delta . D_m$ [۲۹]. روش پیشنهادی در الگوریتم ۱ خلاصه شده است.

الگوریتم ۱: الگوریتم پیشنهادی

Require:

K: *Perfect field with characteristic prime number of p ;*
C: *Equation of Hyperelliptic curve 'C' over perfect field K;*
P: *Point P on the curve C;*
δ : *4- bit Key.*

Ensure:

Sb_i : *Dynamic S-Box i.*

Begin

1: Calculate $D_m = \sum_{p\in c} m_p \,.P$
2: Calculate $D_n = \delta.\, D_m$
3: Calculate $D_m + D_n = \sum_{p\in c} m_p \,.P + \sum_{p\in c} n_p \,.P = \sum_{p\in c}(m_p + n_p)\,.P = (x_p, y_p)$
4. Obtain $Q = x_p \oplus y_p$
4. Represent Q in hexadecimal form
5. Extract n unique bits from Q into 16 hex digits of 4-bits
6. The outcome is Sb_1 which is 64 bits long
6. To obtain the next N dynamic S-Boxes
For i=1 to N
Sb_i= Shift S-Box Sb_1, 4-bits towards left circularly.

End.

مثال ۲: اگر در میدان کامل K ، مقدار مشخصه برابر با $p = 10^{34} + 1233$ باشد، در معادله $y^2 = x^5 + 2x^2 + x + 3$، دو نقطه P_1 و P_2 را برای محاسبه D_m انتخاب می‌کنیم. علاوه بر این، یک کلید برای D_n تولید می‌کنیم و S-Box تولید می‌شود:

P_1 = [280269558793776638909191002790764 0, 177427076027039770261572543921716]
P_2 = [100000000000000000000000000001231, 131261331295864003521648725458531 1]
Key = 23534739862384236842
S-Box = [1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0]

در روش پیشنهادی، برای به دست آوردن S-Boxهای بعدی، در داخل یک حلقه for، از عمل شیفت چرخشی ۴ بیت به سمت چپ استفاده می‌کنیم.

۵- ارزیابی کارایی روش پیشنهادی

در این بخش ، اثربخشی روش پیشنهادی از طریق چهار معیار شامل دو سویی بودن، اثر فرو پاشی بهمنی، غیرخطی بودن و درجه جبری ارزیابی می شود. سپس نتایج به دست آمده با توجه به معیارهای ذکر شده ارائه می‌شود.

۵-۱- معیارهای ارزیابی

عملکرد الگوریتم پیشنهادی S-Box با استفاده از معیارهای زیر ارزیابی می شود [۸]:

الف) دو سوئی بودن تابع: تابع دوسوئی $f: A \rightarrow B$ ، یک نگاشت یک به یک و پوشا از اعضای مجموعه A به اعضای مجموعه B است.

ب) اثر فروپاشی بهمنی: یک تابع، اثر فروپاشی بهمنی را ارضا می‌کند زمانی که با تغییر در یک بیت در ورودی، باعث ایجاد تغییر در بیت خروجی با احتمال ۵۰٪ شود.

ج) غیر خطی بودن: S-Box تولید شده باید ماهیتی کاملاً غیرخطی داشته باشد که بتواند فرایند تجزیه و تحلیل رمزنگاری را کاملاً دشوار کند. فرض کنید $ax + \partial$مجموعه ای از تمام توابع ترکیبی باشد که در آن $a \in F_2^n$ و $\partial \in F_2$.

همچنین، فرض کنید $b.F = b_1 f_1 + \cdots + b_n f_n$ یک ترکیب خطی از توابع بولین f_i از F است که در آن $b = (b_1, \ldots b_1) \in F_2^n$, غیر صفر است. غیرخطی بودن (NL) برای یک S-Box به شکل معادله ۵ تعریف می‌شود [۳۰]:

$$NL(F) = \min\, d_H\,(b.F(x), a.x + \partial) \qquad (۵)$$

غیرخطی بودن یک S-Box با اندازه $n.m$، حداقل فاصله همینگ بین مجموعه تمام ترکیبات خطی غیر ثابت از توابع مولفه F و مجموعه تمام توابع ترکیبی روی F_2^n است.

د) درجه جبری: درجه یک تابع بولین درجه‌ای از بزرگترین تابع تک جمله‌ای در فرم نرمال جبری آن است. S-Box باید درجه جبری بالایی داشته باشد. S-Box با درجه پایین، به حملات حساس است.

چند دستور Sage جهت محاسبه درجه جبری SMS4 به این قرار است:

```
Sage= from sage.crypto.sbox import SBox
Sage=SBox [0xc,0x5,0x6,0xb,0x9,0x0,0xa,0xd,0x3,0xe,0xf,
0x8,0x4,0x7,0x1,0x2])
sage: S.min_degree()
sage: S.max_degree()
```

در این مقاله، مجموعه‌ای از آزمایشات با استفاده از SageMath جهت ارزیابی عملکرد الگوریتم پیشنهادی S-Box انجام شده است .طرح پیشنهادی با الگوریتم SMS4 در [۱۷] مقایسه شده است. محاسبات انجام شده جهت ارزیابی روش پیشنهادی، با دو کلید مختلف انجام شده است و نتایج در جدول ۲ نشان داده شده است.

جدول ۲. مقایسه نتایج ارزیابی S-Box پیشنهادی و SMS4

الگوریتم	خیر خطی بودن	حداقل درجه جبری	حداکثر درجه جبری
SMS4	۴	۲	۳
S-Box پیشنهادی	۴	۴	۴

با توجه به نتایج به دست آمده، چهار معیار ارزیابی دو سویی بودن، اثر فرو پاشی بهمنی، غیرخطی بودن و درجه جبری الگوریتم پیشنهادی بررسی می‌شود.

الف) دو سوئی بودن الگوریتم پیشنهادی:

در S-Box وابسته به کلید پویای پیشنهادی، نگاشت یک به یک و پوشا، از بردارهای ورودی به بردارهای خروجی وجود دارد، زیرا بردارهای ورودی و بردارهای خروجی ایزومورف هستند. بنابراین معیار دو سوئی بودن برای S-Box وابسته به کلید پویا پیشنهادی برآورده شده است.

ب) اثر فروپاشی بهمنی الگوریتم پیشنهادی:

در الگوریتم پیشنهادی، تغییرات جزئی در بردار ورودی منجر به تغییر چشمگیر در بردار خروجی می‌شود. S-Box برای کلیدهای ۲۳۵۳۴۷۳۹۸۶۲۳۸۴۲۳۶۸۴۳ و ۲۳۵۳۴۷۳۹۸۶۲۳۸۴۲۳۶۸۴۲ (باتغییر یک بیت) [۱، ۱، ۱، ۰، ۰، ۰، ۰، ۰، ۱، ۰، ۰، ۰، ۰، ۰، ۱، ۱، ۱، ۰، ۰، ۰، ۰، ۰، ۱، ۰، ۱، ۰، ۰، ۰، ۱، ۰، ۱، ۰، ۱، ۰، ۰، ۰، ۱، ۰، ۱، ۰، ۱، ۰، ۰، ۰، ۱، ۰، ۱، ۰، ۱، ۰، ۰، ۰، ۱، ۰، ۱، ۰، ۱، ۰، ۰، ۰، ۱، ۰، ۱، ۰، ۱، ۰، ۰، ۰] است و از این رو بطور قابل توجهی S-Boxهای مختلفی تولید می‌شوند. بنابراین فروپاشی بهمنی در کلید پویا وابسته به کلید S-Box پیشنهادی وجود دارد و کامل است.

ج) غیر خطی بودن الگوریتم پیشنهادی:

از آنجا که کلیدهای پویای وابسته به S-Boxها کاملاً تصادفی از کلید تولید می‌شوند، هر S-Box دارای خصوصیت غیرخطی نسبتاً بالایی است و احتمال کامل بودن آن بالاست. غیرخطی بودن الگوریتم پیشنهادی در جدول ۲ نشان داده شده است. در [۳۱] ، نویسندگان اظهار داشتند که غیرخطی بودن باید به بهترین غیرخطی شناخته شده نزدیک باشد (به عنوان مثال، مانند NL=۴ که توسط

SMS4 S-Box بدست آمده). بنابراین، در این مقاله، ۳ < NL را برای S-Box بدست آمده که از نظر رمزنگاری، درطبقه قوی قرار می‌گیرد.

د) درجه جبری الگوریتم پیشنهادی:

نتایج بدست آمده نشان می‌دهد که در الگوریتم پیشنهادی، مقدار درجه جبری برابر با ۴ است که عملکرد بهتری نسبت به الگوریتم SMS4 از خود نشان می‌دهد.

۶- نتیجه‌گیری

بخش اصلی هر روش رمزنگاری کلید متقارن، S-Box است که با چالش‌هایی مواجه است. در اکثر الگوریتم‌های رمزنگاری، S-Box ثابت است. چالش این مقاله، چگونگی تضمین کارایی S-Box تولید شده در دستگاه‌های پویای اینترنت اشیا با منابع محدود است. در طرح پیشنهادی، از خم ابر بیضوی برای تولید S-Box استفاده شد و نیز ارزیابی الگوریتم پیشنهادی با استفاده از ابزار Sage انجام پذیرفت. با توجه به ارزیابی‌های انجام شده این نتجه حاصل شد که طرح پیشنهادی برای تولید S-Box وابسته به کلید پویا، کلیه معیارهای یک S-Box کارآمدتر را نسبت به SMS4 را برآورده می‌کند.

۷- مراجع

[1] E. Biham, and A. Shamir, *Differential cryptanalysis of the data encryption standard*: Springer Science & Business Media, 2012.

[2] P. Asghari, A.M. Rahmani, and H. Haj Seyyed Javadi, "A medical monitoring scheme and health-medical service composition model in cloud-based IoT platform," *Transactions on Emerging Telecommunications Technologies* , vol. 30, no. 6, pp. e3637, 2019.

[3] S. Singh, , P.K. Sharma, S.Y. Moon, and J.H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions" *Journal of Ambient Intelligence and Humanized Computing* pp. 1-18, 2017.

[4] C. Wang, J. Shen, Q. Liu, Y. Ren, and T. Li. "A novel security scheme based on instant encrypted transmission for internet of things," *Security and Communication Networks,* 2018.

[5] M. Elhoseny, G. Ramírez-González, O.M. Abu-Elnasr, Sh.A. Shawkat, N. Arunkumar, and A. Farouk. "Secure medical data transmission model for IoT-based healthcare systems." *Ieee Access,* vol. 6, pp. 20596-20608, 2018.

[6] K. McKay, , B. Lawrence, S.T. Meltem, and M. Nicky, *Report on lightweight cryptography*. No. NIST Internal or Interagency Report (NISTIR) 8114 (Draft): National Institute of Standards and Technology, 2016.

[7] I.K. Dutta, B. Ghosh, and M. Bayoumi, "*Lightweight Cryptography for Internet of Insecure Things: A Survey*," *IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, 2019.

[8] J. Daemen, , and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard:* Springer Science & Business Media, 2013.

[9] M. Babu, and G.A. Sathish Kumar, "In Depth Survey on SMS4 Architecture," *International Conference on Intelligent Computing and Communication for Smart World (I2C2SW)*, IEEE, pp. 33-36, 2018.

[10] D. Dinu, , Y. Le Corre, D. Khovratovich, L. Perrin, J. Großschädl, and A. Biryukov, "Triathlon of lightweight block ciphers for the internet of things," *Journal of Cryptographic Engineering*, vol. 9, no. 3, pp. 283-302, 2019.

[11] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems." *Neural Computing and Applications*, vol. 31, no. 8 pp. 3317-3326, 2019.

[12] S.H. Erfani, , H.HS Javadi, and A.M. Rahmani, "A dynamic key management scheme for dynamic wireless sensor networks," *Security and Communication Networks*, vol 8, no. 6, pp. 1040-1049, 2015.

[13] A. Prathiba, and V. S. Bhaaskaran, "Lightweight S-box architecture for secure internet of things," *Information*, vol. 9, no. 1, pp. 13, 2018.

[14] S. Singh, , P.K. Sharma, S.Y Moon, and J.H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing* , pp. 1-18, 2017.

[15] N. Koblitz, "Hyperelliptic cryptosystems." *Journal of cryptology* , vol. 1, no. 3, pp. 139-150, 1989.

[16] D. Mukhopadhyay, A. Shirwadkar, P. Gaikar, and T. Agrawal, "Securing the data in clouds with hyperelliptic curve cryptography," *IEEE International Conference on Information Technology*, pp. 201-205, 2014.

[17] W. A. Stein, "Sage Mathematics Software (Version 4.8. 0) The Sage Development Team, " 2012.

[18] T. Ara, P.G. Shah, and M. Prabhakar, "Dynamic key dependent S-Box for symmetric encryption for IoT devices," *Second International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, IEEE, pp. 1-5, 2018.

[19] T.W. Cusick, and P. Stanica, *Cryptographic Boolean functions and applications*: Academic Press, 2017.

[20] A. J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, "Applied cryptography." *CRC, Boca Raton*, 1996.

[21] J. Chandrasekaran, B. Subramanyan, and Raman Selvanayagam. "A chaos based approach for improving non linearity in S box design of symmetric key cryptosystems," *International Conference on Computer Science and Information Technology*, pp. 516-522, Springer, Berlin, Heidelberg, 2011.

[22] MD A. Mushtaque, H. Dhiman, Sh. Hussain, and Sh.i Maheshwari, "Evaluation of DES, TDES, AES, blowfish and two fish encryption algorithm: based on space complexity," *International Journal of Engineering Research & Technology (IJERT)*, vol. 3, no. 4, pp. 283-286, 2014.

[23] G. Jacob, A. Murugan, and I. Viola, "Towards the Generation of a Dynamic Key-Dependent S-Box to Enhance Security," *IACR Cryptol. ePrint Arch, pp.* 92, 2015.

[24] J. Juremi, , R. Mahmod, and S. Sulaiman, "A proposal for improving AES S-box with rotation and key-dependent," *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, IEEE, pp. 38-42, 2012.

[25] F. Y. Mohammad, A. E. Rohiem, and A.D. Elbayoumy, "A novel S-box of AES algorithm using variable mapping technique." *International Conference on Aerospace Sciences and Aviation Technology*, , vol. 13, no. AEROSPACE SCIENCES & AVIATION TECHNOLOGY, ASAT-13, May 26–28, The Military Technical College, pp. 1-10, 2009.

[26] A. Alabaichi, and A. I. Salih, "Enhance security of advance encryption standard algorithm based on key-dependent S-box," *Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*, IEEE, pp. 44-53, 2015.

[27] E. M. Mahmoud, A. Abd, T.A.E. El Hafez, and T. A. El Hafez. "Dynamic AES-128 with key-dependent S-box,", 2013.

[28] N. Koblitz, *Algebraic aspects of cryptography*, Springer Science & Business Media, vol. 3, 2012.

[29] H. CA Van Tilborg, and S. Jajodia, eds. *Encyclopedia of cryptography and security*, Springer Science & Business Media, 2014.

[30] H. Isa, N. Jamil, and M.R. Z'aba, "Construction of cryptographically strong S-boxes inspired by bee waggle dance," *New generation computing*, vol. 34, no. 3, pp. 221-238, 2016.

[31] C. Carlet, "On known and new differentially uniform functions," *Australasian Conference on Information Security and Privacy*, pp. 1-15, Springer, Berlin, Heidelberg, 2011.

پروانه اصغری عضو هیئت علمی تمام وقت و استادیار گروه مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد تهران مرکزی است. او دوره کارشناسی خود را در رشته مهندسی کامپیوتر نرم افزار از دانشگاه صنعتی شریف، کارشناسی ارشد خود در رشته مهندسی کامپیوتر نرم افزار، از دانشگاه علم و صنعت، و دکترای خود را در رشته مهندسی کامپیوتر از دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران، به اتمام رساند. زمینه تحقیقاتی وی در حوزه سیستم‌های توزیع شده، اینترنت اشیا، رایانش ابری و محاسبات سرویس گرا است. آدرس پست الکترونیکی ایشان عبارت است از:

p_asghari@iauctb.ac.ir

سید حمید حاجی سید جوادی مدرک تحصیلی کارشناسی، کارشناسی ارشد و دکتری خود را در دانشگاه صنعتی امیرکبیر، تهران، ایران دریافت نمود. وی به عنوان عضو هیئت علمی تمام وقت و استاد تمام در گروه ریاضیات و علوم کامپیوتر دانشگاه شاهد، تهران، مشغول به کار است. زمینه‌های تحقیقاتی وی جبر کامپیوتر ، شبکه‌های حسگر بیسیم، اینترنت اشیا، رمزنگاری و امنیت است. آدرس پست الکترونیکی ایشان عبارت است از:

h.s.javadi@shahed.ac.ir

---

[1] Hyperelliptic curve
[2] Bijection
[3] Bijection
[4] Strict Avalanche Effect
[5] Algebraic Degree
[6] End-to-end
[7] Stream and block cipher
[8] Advanced-Encryption-Standard
[9] Data-Encryption-Standard
[10] Substitution box
[11] Wireless Body Area Network (WBAN)
[12] RFID Wireless Sensor Network (RFID WSN)
[13] Hyperelliptic curve
[14] genus
[15] Lightweight Block Ciphers (LwBC)
[16] Lightweight Hash Functions (LwHF)
[17] Lightweight Stream Ciphers (LwSC)
[18] Plain text
[19] Cipher text
[20] code-word
[21] rotation
[22] linear feedback shift register
[23] Hyperelliptic Curve-Discrete-Logarithm-Problem

The CSI Journal on Computing Science and Information Technology
Vol. 18, No.2, 2021

Lightweight Key-Dependent Dynamic S-Boxes based on Hyperelliptic Curve for IoT Devices

Parvaneh Asghari [1], Seyyed Hamid Haj Seyyed Javadi [2]

[1] Department of Computer Engineering, Islamic Azad University Central Tehran Branch, Tehran, Iran
2 Department of Mathematics and Computer Science, Shahed University, Tehran, Iran

Abstract

Security is one of the main issues in the Internet of Things (IoT). Encryption plays a curtail role in making these systems secure. Substitution Box (S-Box) has an effective impact on block encryption methods. Due to the restricted resource capacities of IoT nodes, providing a lightweight S-Box is a challenging problem. This paper presents a key-dependent S-Box using the Hyperelliptic curve. The proposed S-Box is analytically evaluated using performance criteria including bijection, nonlinearity, strict avalanche effect, and algebraic degree. The evaluation results endorse that the offered S-Box production algorithm is a considerably effective way to generate strong cryptographic S-Box.

Keywords: Dynamic S-Box; Hyperelliptic curve; Block ciphers; IoT Security